**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 06**

**IT Security**

**Password**

Password atau kata sandi adalah sebuah cara untuk memastikan bahwa orang yang akan masuk pada sebuah system adalah benar benar orang yang berhak. Sebuah sistem akan meminta tanda pengenal dari pengguna, apabila pengguna ingin masuk ke dalam system tersebut. Salah satu cara sebuah system mengenali pengguna adalah dengan menggunakan password dan user name.

Serangan dengan menggunakan password untuk masuk ke sebuah system secara illegal dapat di kategorikan menjadi tiga kelompok, yaitu:

1. Coba coba atau brute force.

Seorang hacker menggunakan program komputer atau script untuk mencoba login dengan kemungkinan kombinasi password, biasanya dimulai dengan password yang paling mudah ditebak. Selain itu seorang hacker juga berpikir: jika seorang memiliki daftar perusahaan, ia dapat dengan mudah menebak username dan ada kemungkinan salah satu pengguna system dari daftar tersebut masih menggunakan "password123" atau “p@$$w0rd”.

2. Dictionary Attack

Seorang hacker menggunakan program atau skrip untuk mencoba untuk login dengan mencoba coba melalui kombinasi dari kata-kata umum. "Berbeda dengan serangan brute force, di mana sebagian besar password dicari secara sistematis, dictionary attack (serangan kamus) mencoba hanya dengan kemungkinan yang paling mungkin berhasil, biasanya berasal dari daftar kata misalnya kamus. Umumnya, serangan kamus berhasil karena banyak orang memiliki kecenderungan untuk memilih password yang pendek (7 karakter atau kurang), seperti kata-kata tunggal yang ditemukan dalam kamus atau kata sederhana, mudah diprediksi variasi pada kata-kata, seperti menambahkan digit."

3. Key logger attack

Seorang hacker menggunakan program untuk melacak semua keystrokes pengguna. Sebuah serangan logger kunci berbeda dari bruteforce atau serangan kamus dalam banyak cara. Program pencatatan kunci password (key logger) yang banyak digunakan adalah malware (atau virus full-blown). Malware ini harus terinstall pada perangkat pengguna (sering pengguna tertipu untuk men-download dengan mengklik link dalam email). Serangan logger kunci juga berbeda dengan brute force dan dictionary attack karena password yang kuat tidak memberikan banyak perlindungan terhadap peralatan atau system yang sudah terinfeksi key logger. Hal inilah yang merupakan salah satu alasan bahwa multi-faktor otentikasi (MFA) menjadi yang harus dimiliki untuk semua bisnis dan organisasi.

Dengan otentikasi multi-faktor (juga disebut otentikasi dua faktor, 2FA), pengguna diwajibkan untuk tidak hanya memberikan password untuk mendapatkan akses ke sistem, tetapi juga keamanan lain, seperti yang unik kode akses-waktu (token) yang dihasilkan dari perangkat atau aplikasi mobile di smartphone. Sebuah jaringan yang dilindungi oleh MFA hampir tak tertembus untuk serangan luar; bahkan jika hacker dapat mencapai password sistem, ia tidak akan mampu menembus faktor keamanan kedua ini.

Kita semua pernah mendengar peringatan tentang keamanan password. Jangan pernah berbagi password Anda. Jangan pernah menggunakan password bawaan vendor (seperti Admin). Jangan pernah menggunakan password yang mudah ditebak (seperti p@$$w0rd atau 123456). Tidak peduli apa industri Anda bekerja, Anda pasti mendengar tentang password bahkan ada aturan untuk membuat password ini pada pekerjaan Anda. Akhir akhir ini sering kali kita mendengar masalah keamanan, seperti penggunaan kartu kredit orang lain untuk belanja online, yang salah satunya disebabkan oleh password.

Kita dapat belajar dan mengetahui beberapa jenis serangan yang menggunakan keahlian teknis untuk menyusup sistem komputer yang telah dilindungi oleh peralatan canggih. Untuk mempertahankan system network di perusahaan kita dengan peralatan canggih, memerlukan biaya yang tidak sedikit. Tetapi tetap saja, dengan menerapkan teknologi terbaru dan tercanggih bukan menjadi jaminan jaringan kita terbebas dari serangan atau penyusupan.

Ada jenis lain dari penyerang yang bisa menggunakan taktik untuk menggunakan kelemahan manusia. Mereka adalah ahli ahli sosial yang mengeksploitasi kelemahan psikologi manusia. Mereka menggunakan berbagai media, termasuk panggilan telepon dan media social. Penyerang langsung menanyakan user name dan password. Ada beberapa jenis serangan dengan menggunakan social engineering ini, yang paling adalah phishing, dalih, umpan, quid pro quo dan Tailgating.

Penipuan phishing mungkin jenis yang paling umum dari serangan social engineering yang digunakan saat ini. Kebanyakan penipuan phishing menunjukkan karakteristik sebagai berikut: Mencoba untuk mendapatkan informasi pribadi, seperti nama, alamat dan nomor kartu kredit atau informasi rahasia lainnya. Biasanya mereka menggunakan tautan atau embed link yang mengarahkan pengguna ke situs web yang terlihat tampak sah, tetapi sebenarnya web buatan si penyerang.

Pretexting adalah bentuk lain dari social engineering dimana penyerang membuat scenario yang kelihatannya baik bagi taget, dengan cara ini mereka mencoba untuk mendapatkan informasi pribadi korban atau target. Hal ini bisa terjadi melalui telepon atau email. Jenis-jenis serangan yang umum adalah mengambil bentuk dari scammer yang berpura-pura bahwa mereka membutuhkan informasi tambahan dari target untuk mengkonfirmasi identitas mereka.

Baiting atau umpan adalah mirip dengan serangan phishing. Namun, yang membedakan dari social engineering yang lainnya adalah janji memberikan hadiah baik berupa barang atau uang untuk memikat korban. Baiters mungkin akan menawarkan pengguna atau target berupa musik gratis atau film yang dapat di download, jika korban mau memberitahukan informasi rahasia ke situs tertentu. Informasi rahasia dapat berupa user name, password atau nomor kartu kredit. Serangan semacam ini tidak terbatas pada skema online, penyerang juga dapat memanfaatan keingintahuan manusia melalui penggunaan media fisik. Salah satu bentuk serangan ini bisa dalam bentuk pembagian flash disk gratis, begitu flash disk ini di colokan ke usb di computer maka akan menginstall keylogger.

**Personal Security Defenses**

Untuk mencegah serangan terhadap system computer atau system network selain password dan antivirus, yang harus diperhatikan lagi adalah semua aplikasi atau software yang terinstall pada computer kita, termasuk operating sistemnya.

Update software adalah hal yang paling penting untuk dilakukan termasuk update operating system. Microsoft window mempunyai beberapa option untuk update, yaitu: automatic, download, notify dan turnoff. Untuk alasan keamanan sebaiknya kita dapat memilih automatic. Patch pada operating dan software yang lainnya sangatlah penting untuk memperbaiki vulnerability yang ada pada software tersebut. \

Demikian juga untuk antivirus sebaiknya di set automatic update. Update antivirus umumnya adalah untuk mengupdate database ciri ciri unik dari virus virus. Antivirus bekerja berdasarkan mencari ciri ciri unik virus yang ada di file atau data yang masuk ataupun keluar dari system computer.

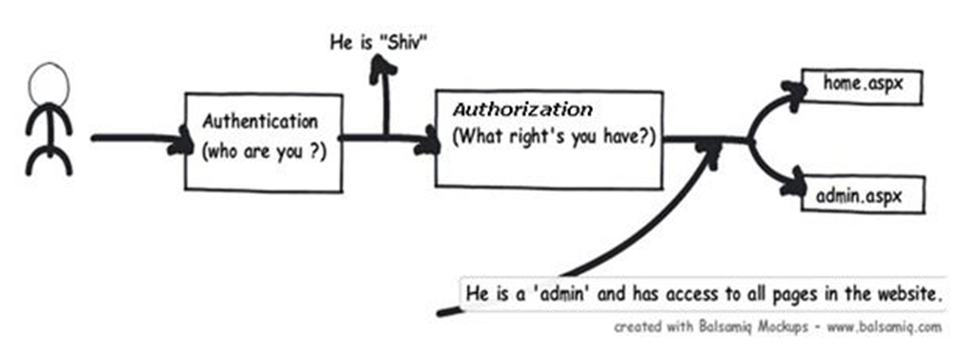
Selain melakukan pencegahan untuk perangkat lunak, pencegahan dalam hal perangkat keras juga sangat penting. Misalnya gunakanlah kunci laptop apabila laptop ditinggal untuk suatu waktu tertentu. Untuk area server, gunakan kunci yang tidak mudah dibuka dengan teknik umum, dan gunakan akses list sehingga hanya orang orang tertentu saja yang mendapatkan akses ke ruang server.

**Authentication dan Authorization**

Sebenarnya authentication dan authorization adalah konsep yang sudah lama tetapi masih sangat berguna hingga saat ini, tetapi cara atau teknik authentication dan authorization berkembang menyesuaikan dengan perkembangan teknologi saat ini.

Otentikasi adalah proses verifikasi identitas pengguna dengan menggunakan semacam kepercayaan (kredensial) dan menggunakan kredensial untuk memverifikasi identitas pengguna. Jika kredensial valid, proses otorisasi dimulai. Hasil proses otentikasi selalu diikuti oleh proses otorisasi, seperti yang terlihat pada gambar 1.

Otorisasi adalah proses yang memungkinkan suatu pengguna dikonfirmasi untuk mengakses sumber daya dengan memeriksa apakah pengguna memiliki hak akses ke sistem. Otorisasi membantu untuk mengontrol hak akses dengan memberikan atau menolak izin khusus untuk pengguna. Seperti yang terlihat pada gambar 2.



Gambar 1. Proses otentikasi

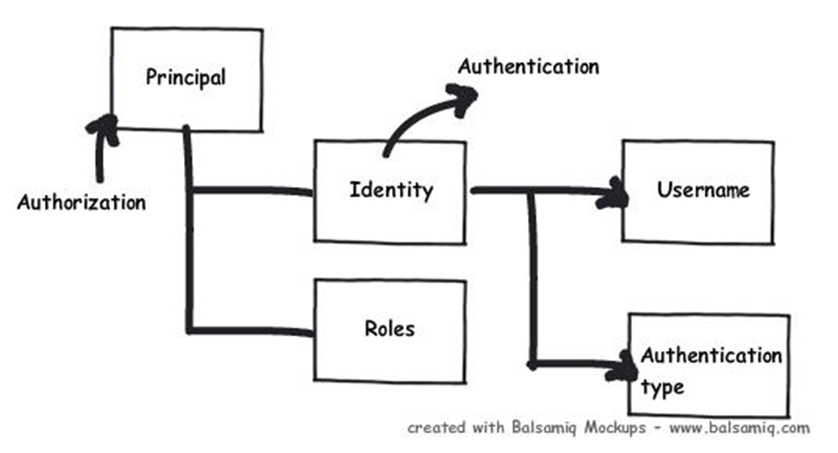
Dalam proses otentikasi dapat dibagi menjadi tiga grup, yaitu:

• What do you know? Adalah proses otentikasi dengan menggunakan apa yang diketahui oleh pengguna. Contoh penggunaan user name dan password

• What do you have? Adalah proses otentikasi dengan menggunakan sesuatu yang dimiliki oleh pengguna. Contoh penggunaan adalah kartu karyawan untuk tapping absen

• Who are you? Adalah proses otentikasi dengan menggunakan keunikan yang dipunyai oleh setiap orang. Contoh penggunaan sidik jari, retina mata dan voice recognition.

Untuk memperkuat otentikasi, sebaiknya digunakan dua teknik otentikasi, misalnya what do you know dengan what do you have. Contohnya pada saat log in kesebuah website bank, pertama harus memasukkan user name dan password atau menggunakan teknik what do you know, kemudian saat melakukan transaksi harus menggunakan token dengan memasukkan angka yang ada di token pada website atau menggunakan teknik what do you have. Dengan menggunakan dua cara otentikasi yang berbeda ini maka dapat meningkatkan keamanan dalam hal otentikasi. Menggunakan dua cara otentikasi dikenal dengan 2FA atau Two Factor Authentication. Contoh yang lain adalah pada penggunaan mesin ATM, kita menggunakan kartu ATM dan Pin, yang artinya menggunakan metode what do you have yaitu kartu ATM dan what do you know yaitu nomor pin.



Gambar 2. Proses otorisasi

**SIMPULAN**

1. Dictionary attack adalah sebuah cara yang paling popular untuk mendapatkan cracking password.
2. Sebaiknya pilihlah password yang tidak ada di kamus, atau buatlah password dengan dua atau tiga kata.

**DAFTAR PUSTAKA**

1. Stallings, William. (2006). Cryptography and Network Security. 4th edition. Pearson Education.Whitman, M.E., Mattoro, H.J. (2013).
2. Scambray, Joel; Liu, Vincent; Sima, Caleb. (2011). Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd Edition. McGraw-Hill. ISBN: 9780071740647.
3. Slay, Jill and Andy Koronios. (2006). Security and Risk Management. John Wiley & Sons, Inc.